REFRAMING PRIVACY 2.0 IN ONLINE SOCIAL NETWORKS

Heng Xu[*]

I. INTRODUCTION

With the booming popularity of Online Social Networks ("OSNs"), a tremendous number of users share personal information, activities, opinions, photos, and videos on OSNs, which is giving rise to growing privacy concerns among various stakeholders, including providers of OSNs, marketers, and other users on the social networking sites. OSNs brought the voluntary disclosure of personal data to the mainstream, thus exposing users' published information with potential abuse.[1] Privacy concerns pertain to the acquisition of personal data and the potential risks that users may experience over the possible privacy breaches.[2] At the same time, despite the presence of some privacy norms and regulations, there are relatively few well-established institutional rules and contracts governing OSNs, which gives rise to opportunism.

An additional dimension that represents the complexity of studying privacy risks in the context of OSNs is added by the highly dynamic social interactions with rich data exchange. Users are actively creating content that not only reveals their own identities but also connects with their "friends" (e.g., tagging a friend in an image or linking to a friend's personal profile in a wall post). Such interpersonal nature of data sharing activities raises some new privacy challenges because users and their social ties share responsibilities for

* Assistant Professor of Information Sciences and Technology, The Pennsylvania State University. I wish to thank the Board of the *Journal of Constitutional Law* for their valuable editing assistance. I also gratefully acknowledge the financial support of the National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

1 *See* Spencer Kelly, *Identity 'at Risk' on Facebook*, BBC NEWS (May 1, 2008), http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm (explaining how seemingly innocuous Facebook applications can collect personal user details without the user knowing).

2 *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE (2004), *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf (discussing common online consumer privacy concerns).

keeping their shared data safe and private. Even if some users think they have tight privacy settings, their personal information could be accessed or misused by unauthorized parties due to their friends' ignorance of privacy and security.[3] The need for collective privacy management arises due to the inability to monitor others on the network and uncertainty about their behaviors.

To address the acute concerns for collective information privacy in the context of OSNs, this Article aims to add to the growing privacy literature by exploring conceptual underpinnings of privacy in the context of OSNs, identifying privacy management strategies, and discussing major drivers and impediments of information disclosure. This Article contributes to existing privacy research in several important ways. First, rather than drawing on a single theoretical lens, I try to build upon previous literature from multiple theoretical lenses to create a common understanding of individuals' information disclosure or withholding behavior in the context of OSNs. The synthesis of privacy literature, bounded rationality theory, control agency theory, and social contract theory may provide a rich understanding of the major drivers and impediments of information disclosure in the context of OSNs.

Second, although several studies have reported growing privacy concerns,[4] recent research has identified the phenomenon of "privacy paradox" that individuals express privacy worries but behave in ways that contradict their statements.[5] In the context of OSNs, such a privacy attitude/behavior dichotomy is more apparent. While "inva-

---

3 Na Wang et al., *Third-Party Apps on Facebook: Privacy and the Illusion of Control*, *in* PROCEEDINGS OF THE 5TH ACM SYMPOSIUM ON COMPUTER HUMAN INTERACTION FOR MANAGEMENT OF INFORMATION TECHNOLOGY (2011), *available at* http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags-CHIMIT11.pdf ("If the user is not diligent about setting secure privacy settings, the apps may be able to access his/her friends' information. This is especially unfair for his/her friends who may be proactive and try to make smart privacy choices.").

4 Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PET (2006), *available at* http://dataprivacylab.org/dataprivacy/projects/facebook/facebook2.pdf (citing "privacy policy" as a "highly important issue in the public debate by our respondents" (internal quotation marks omitted)); Christopher M. Hoadley et al., *Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry*, 9 ELECTRONIC COM. RES. & APPLICATIONS 50, 55 (2010) (discussing users' perceptions that easier access to information leads to a decrease in one's control over personal information).

5 Acquisti, *supra* note 2, at 1 ("Even privacy concerned individuals are willing to trade-off privacy for convenience, or bargain the release of very personal information in exchange for relatively small rewards."); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SEC. & PRIVACY, Jan./Feb. 2005, at 26, 29 ("[R]ecent surveys, anecdotal evidence, and experiments have highlighted an apparent dichotomy between privacy attitudes and actual behavior.").

sion of privacy" shockwaves flood the headlines of newspapers, allegedly "angry users" are still uploading their work histories to LinkedIn, or their photos to Flickr, or updating their relationship statuses to Facebook, choosing to connect their online identities with these key pieces of personal information. This Article contributes to this controversial issue by addressing the inconsistencies in individual privacy decisions from the bounded rationality and optimistic bias theoretical perspectives.

In what follows, the Article begins with a discussion of the conceptual underpinnings of privacy in the context of OSNs. Next, the control agency theory in the psychology literature is applied in order to identify privacy management strategies. The impacts of trust in OSNs providers and trust in social ties are also examined. Important postulates from theories in bounded rationality, optimistic bias, control agency, and social contract are synthesized into a theoretical framework. The Article concludes with a discussion of theoretical and practical implications.

II. PRIVACY: A MULTIFACETED CONCEPT

Various definitions of privacy have been given in the literature. The conceptualizations of privacy range from a "right to be let alone" in law,[6] to a "state of limited access" in philosophy,[7] to the control over information about one's self in social sciences.[8] Such a variety of conceptualizations of privacy leads Solove to note that privacy is "in disarray," and "[n]obody can articulate what it means."[9] Numerous efforts have been devoted by privacy scholars to develop a consistent conceptualization of privacy and bring together the different perspectives.[10]

---

6 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (internal quotation marks omitted).

7 Ferdinand David Schoeman, *Preface* to PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 3 (Ferdinand David Schoeman ed., 1984).

8 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

9 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006).

10 *See generally* Giovanni Iachello & Jason Hong, *End-User Privacy in Human-Computer Interaction*, 1 FOUNDS. & TRENDS IN HUMAN-COMPUTER INTERACTION 1, 1–137 (2007), *available at* http://www.cs.cmu.edu/~jasonh/publications/fnt-end-user-privacy-in-human-computer-interaction-final.pdf (summarizing research on privacy in Human-Computer Interaction and charting future research trends while noting areas that are "timely but lagging"); Clinton D. Lanier, Jr. & Amit Saini, *Understanding Consumer Privacy: A Review and Future Directions*, 12 ACAD. OF MARKETING SCI. REV., no. 2, 2008, at 1–48, *available at* http://www.kommunikationsforum.dk/Profiler/ProfileFolders/Kkort/Understanding.pdf (providing a general understanding on the concept of privacy while reviewing literature on consumer privacy and suggesting future research directions that will expand the

The prior body of conceptual exploration has led to welcome efforts to synthesize various perspectives and identify common ground. Toward this end, Solove describes privacy as "a shorthand umbrella term" for a related web of privacy problems resulting from information collection, processing, dissemination, and invasion activities.[11] He discusses what conditions reduce privacy by developing a taxonomy of information processing and dissemination activities, which maps out various types of problems and harms that constitute privacy violations. Solove's groundwork for a pluralistic conception of privacy differentiates the concept of privacy (as an individual state) from the management of privacy (arising from organizational information processing activities).[12] In this Article, rather than drawing on a monolithic concept of privacy from a single theoretical lens, I attempt to integrate multiple theoretical lenses to develop a common understanding of information privacy in the context of OSNs.

A. Privacy as Control vs. Privacy as Restricted Access

Relating information privacy to the control of personal information is an important perspective found in prior literature, which has contributed to and stimulated research on privacy as a control-related concept.[13] Wolfe and Laufer suggested that "[t]he need and ability to exert control over self, objects, spaces, information and behavior is

---

current understanding); H. Jeff Smith, Tamara Dinev & Heng Xu, *Information Privacy Research: An Interdisciplinary Review*, 35 MIS Q. 989–1015 (2011), *available at* http://pal.ist.psu.edu/MISQ.pdf (providing an "interdisciplinary review of privacy-related research in order to enable a more cohesive treatment").

11 Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 760 (2007).

12 *Id.* at 754–60.

13 *See, e.g.*, Irwin Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33 J. SOC. ISSUES, Summer 1977, at 66, 67 (discussing Altman's "conceptualization of privacy as the selective control of access to the self"); Carl Anderson Johnson, *Privacy as Personal Control (1)*, *in* 2 MAN-ENVIRONMENT INTERACTIONS: EVALUATIONS AND APPLICATIONS 83 (Daniel H. Carson ed., 1974) (observing that many behavioral scientists recognize that personal control is central to "[a]ny adequate conceptualization of privacy"); Robert S. Laufer et al., *Some Analytic Dimensions of Privacy*, *in* ARCHITECTURAL PSYCHOLOGY 353, 360–61 (Rikard Küller ed., 1973) (describing control as "a critical element in any conception of privacy," and explaining that "[t]here are at least three aspects of control which are related to privacy: control over choice, control over access, and control over stimulation" (internal quotation marks omitted)); *see also* WESTIN, *supra* note 8, at 7 (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

[a] critical" element in any concept of privacy.[14] This view of control in justifying the concept of privacy is also found in a number of consumer privacy studies.[15] For instance, consumers perceive information disclosure as less privacy-invasive when they believe that they will be able "to control future use of the information."[16] This stream of privacy literature indicates that control should be one of the key factors that "provides the greatest degree of explanation for privacy concern[s]."[17]

While control has received attention as the common core of definitions of privacy, researchers in philosophy and some branches of social science have noted that it is important to distinguish the concept of privacy from the notion of control.[18] "According to DeCew,

---

14 Maxine Wolfe & Robert Laufer, *The Concept of Privacy in Childhood and Adolescence*, *in* 2 MAN-ENVIRONMENT INTERACTIONS: EVALUATIONS AND APPLICATIONS 29, 31 (Daniel H. Carson ed., 1974).

15 *See, e.g.*, Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, J. PUB. POL'Y & MARKETING, Spring 1991, at 149, 149–50 (explaining that "consumer privacy concerns two dimensions," both of which are related to control, and that "control has been included in definitions of privacy offered by" researchers in many fields); Glen J. Nowak & Joseph Phelps, *Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters*, J. DIRECT MARKETING Fall 1997, at 94, 96–97 (observing that "the evolution of the privacy construct suggests that there are at least three conceptualizations that have considerable relevance for direct marketers' consumer information practices," and recognizing that control at least plays a role in the second); Joseph Phelps et al., *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 J. PUB. POL'Y & MARKETING 27, 28–29 (2000) (explaining that privacy "encompasses at least four different dimensions," all of which connect with "information control"); Kim Bartel Sheehan & Mariea Grubbs Hoy, *Dimensions of Privacy Concern Among Online Consumers*, 19 J. PUB. POL'Y & MARKETING. 62, 63 (2000) (explaining that the "predominant influences on the degree to which consumers experience privacy concern" both involve control).

16 Mary J. Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10 ORG. SCI. 104, 106 (1999) (explaining when "individuals are less likely to perceive information collection procedures as privacy-invasive").

17 Sheehan & Hoy, *supra* note 15, at 69.

18 *See, e.g.*, Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 424 (2003) (noting that "[e]ven though control is featured in many privacy theories, few have systematically integrated the control literature into their theories"); Stephen T. Margulis, *Privacy as a Social Issue and Behavioral Concept*, 59 J. SOC. ISSUES 243, 245 (2003) (observing that an earlier definition of privacy Marguils offered, which involved "control over transactions," failed to distinguish between the various types of transactions—transactions limiting access to self, to groups, or to organizations); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1153–55 (2002) (concluding that "[t]he conception of privacy as control over information only partially captures the problem" created by the collection and use of personal information, and arguing for a "bottom-up" conceptualization of privacy); Herman T. Tavani, *Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy*, 38 METAPHIL. 1, 2

we often lose control over information in ways that do not involve an invasion of our privacy."[19] Following such perspective, Waldo et al. argue that "control over information cannot be the exclusive defining characteristic of privacy," and privacy is more than control.[20] Such limitation in the conceptualization of *privacy as control* spurred the formulation of a modified notion of *privacy as restricted access*, which conceptualizes privacy as "[a] condition of limited access to identifiable information about individuals."[21] Tavani and Moor state that "[t]he concept of privacy itself is best defined in terms of restricted access, not control."[22]

In this Article, I argue that neither control nor restricted access perspectives alone can justify the concept of privacy in OSNs. Instead, privacy is a multifaceted concept that should be analyzed with the following considerations: i) degree of control over information release, and ii) degree of ease of information access by others. The event of the Facebook News Feed privacy outcry provided preliminary support for such distinction between perceived control over information release and perceived ease of access: although the Facebook's old (*without* the News Feed features) and new (*with* the News Feed features) "interfaces are isomorphic in terms of actual control over" information release and dissemination, "[t]he introduction of the News Feed . . . enhances the ease of access" to shared data.[23] Hence, it "increases the perceived probability that those data will be accessed by more audiences, which in turn leads to a lower control perception over personal information."[24]

The theoretical distinction between *control over information release* and *ease of information access* seems readily understood. However,

---

(2007) (organizing the "classic . . . philosophical and legal theories of privacy . . . into four broad categories," only one of which explicitly involves control).

19 *See* Solove, *supra* note 18, at 1114 (citing JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 53 (1997)).

20 *See* COMM. ON PRIVACY IN THE INFO. AGE, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 61 (James Waldo et al. eds., 2007). Waldo et al. explain why the notion of "privacy as control" is misleading by presenting a situation where a person chose "to reveal intimate details of his life on national television." *Id.* Based on the notion of "privacy as control," such a person could not claim that a privacy violation has occurred in such a situation (because the person chose to reveal those details). *Id.* But our intuitions would say that this person had less privacy, under a "'privacy as restricted access' theory." *Id.*

21 H. Jeff Smith, *Privacy Policies and Practices: Inside the Organizational Maze*, COMMS. ACM, Dec. 1993, at 104, 106.

22 Herman T. Tavani & James H. Moor, *Privacy Protection, Control of Information and Privacy-Enhancing Technologies*, COMPUTERS & SOC'Y, Mar. 2001, at 6.

23 *See* Hoadley et al., *supra* note 4, at 57.

24 *Id.*

most users in everyday practice may conflate these two dimensions by having an "illusion" of control over the information they reveal: since they have control over the information release, they believe they also have control over others' access to that information.[25] In this Article, I argue that such "illusion" of control could be explained by the *optimistic bias* where users overestimate their control over information release and meanwhile underestimate the future invisible access to their revealed information by others.[26] To provide a richer conceptual description of privacy, this Article demonstrates the theoretical contribution of the *optimistic bias* to the understanding of privacy.

B. Role of Optimistic Bias

The above two perspectives (privacy as control vs. privacy as restricted access) complement each other and reveal different but interrelated approaches to conceptualizing privacy. When looking across these different aspects, I propose that an individual's perceived privacy in the context of OSNs is better viewed as a multifaceted concept that is analyzed with the following considerations:

i) the extent to which users can control the disclosure and dissemination of their personal information (perceived control over information release),

ii) the degree of ease with which their online profiles and their personal information are visible and exposed to others (perceived ease of information access), and

iii) the subjective estimation of control over their information release as well as the future access to their revealed information by others (optimistic bias).

People tend to assign a higher probability for an event with a positive outcome but assign a lower probability for an event with an unfavorable outcome. This phenomenon has been variously referred to as *unrealistic optimism*[27] or *optimistic bias*[28] or *self-favoring bias*.[29] Research

---

25 *See* Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, NINTH WORKSHOP ON ECON. INFO. SECURITY, June 2010, at 1–3 (explaining that their results show that individuals have a false sense of control over others' access to their information when they have control over the publication of their personal information).

26 *See* Neil D. Weinstein & William M. Klein, *Unrealistic Optimism: Present and Future*, 15 J. SOC. & CLINICAL PSYCHOL. 1, 2 (1996) (defining optimistic bias as the tendency to underestimate the "*likelihood* . . . of experiencing negative events").

27 *See* Neil D. Weinstein, *Unrealistic Optimism About Future Life Events*, 39 J. PERSONALITY & SOC. PSYCHOL. 806, 806 (1980) (describing this phenomenon as "unrealistic optimism").

28 *See* Weinstein & Klein, *supra* note 26, at 2 (describing this phenomenon alternatively as "optimistic bias" or "unrealistic optimism").

has shown that individuals demonstrate this optimistic bias when calculating their vulnerability to unfavorable events in various domains such as getting in a car accident[30] or being mugged[31] or being involved in unhealthy behavior.[32] Because measures for estimating the likelihood of an event occurring in the future are not easily obtainable,[33] individuals tend to use a comparative likelihood to evaluate their positions and abilities (e.g., using a peer as comparison target) instead of calculating actual likelihood.[34] With this social comparison process, individuals aim at finding out whether people perceive their risk lower or higher than others' risk, rather than the actual risk. I believe that similar optimistic bias exists in an individual's perception of privacy vulnerability associated with OSNs. As privacy risks are highly subjective and difficult to quantify, users are likely to evaluate their privacy risks by engaging in social comparison process. Therefore, I argue that users on OSNs tend to believe that their privacy risks are lower than that of peers.

In identifying factors that influence optimistic bias in risk perception, researchers have suggested the role of perceived control in influencing the extent of optimistic bias. Perceived control refers to the extent to which a person believes he is capable of "producing desired and preventing undesired events."[35] Similar to risk perception,

---

29 *See* Vera Hoorens, *Self-Favoring Biases for Positive and Negative Characteristics: Independent Phenomena?*, 15 J. SOC. & CLINICAL PSYCHOL. 53, 53 (1996) (observing that this phenomenon is "one of a wide variety of self-favoring biases in social comparison").

30 *See* Frank P. McKenna, *It Won't Happen to Me: Unrealistic Optimism or Illusion of Control?*, 84 BRITISH J. PSYCHOL. 39, 39–41 (1993) (describing research that has found that people underestimate the risk of getting in a car accident in part because people believe themselves to be better-than-average drivers).

31 *See* Linda S. Perloff & Barbara K. Fetzer, *Self-Other Judgments and Perceived Vulnerability to Victimization*, 50 J. PERSONALITY & SOC. PSYCHOL. 502, 503–04 (1986) (describing the results of their study demonstrating the tendency of individuals to underestimate the likelihood of being mugged).

32 *See* Hoorens, *supra* note 29, at 62–63 (describing results of a study demonstrating individuals' tendency to overestimate their likelihood of engaging in healthy behaviors and to underestimate their likelihood of engaging in unhealthy behaviors, relative to an average student).

33 *See* Alexander J. Rothman et al., *Absolute and Relative Biases in Estimations of Personal Risk*, 26 J. APPLIED SOC. PSYCHOL. 1213, 1214 (1996) (observing that risk statistics are "hard to locate" especially for population subgroups).

34 *See* Perloff & Fetzer, *supra* note 31, at 502–03 (observing the tendency of individuals to engage in social comparisons with an average person or peers when estimating the likelihood that a negative life event will occur to them).

35 *See* ELLEN A. SKINNER, PERCEIVED CONTROL, MOTIVATION, AND COPING 8 (1995) (explaining that perceived control can be understood as a need for competence, meaning the ability to control events).

studies have also found a self-serving tendency in personal control perception, which is called "illusion of control."[36]

This illusion of control is documented in various situations. For instance, in daily driving, Svenson found that approximately 80% of drivers among the study participants believe their driving ability is better than average.[37] Accordingly, I argue that such optimistic bias exists in one's perception of information control and information access on OSNs: users tend to perceive themselves to have a higher degree of control over information release and a lower degree of information access than their peers do.

A number of studies have supported the linkage between perceived control and risk perception: on one hand, people show higher comparative optimism and less concern when they believe they can exercise control over potential threats.[38] On the other hand, people perceive themselves as highly vulnerable to dangers when they believe themselves as lacking coping mechanisms.[39] Regarding various privacy threats, if people have a higher level of control beliefs in their information release and in their ability to avoid the potential information access and misuse, then it is reasonable to argue that privacy risk perceptions would be adjusted downward. Furthermore, it appears reasonable to argue that if a person's judgment on his or her ability to control privacy threats is exaggerated, this illusion of control would account for the optimistic bias in his or her risk perception. Thus I argue that the theory of optimistic bias suggests the self-serving tendency in control perception: as individuals' perceived control over their personal information increases, they demonstrate a greater extent of optimistic bias in privacy risk perception. Similarly, the theory of optimistic bias also suggests the self-serving tendency in perceived ease of information access: as users' perceptions of others'

---

36 *See* Ellen J. Langer, *The Illusion of Control*, 32 J. PERSONALITY & SOC. PSYCHOL. 311, 327 (1975) (studying the phenomenon of control illusion and concluding that when certain factors were present, individuals were overly confident and more willing to take risks).

37 Ola Svenson, *Are We All Less Risky and More Skillful than Our Fellow Drivers?*, 47 ACTA PSYCHOLOGICA 143, 146 (1981).

38 Peter Harris, *Sufficient Grounds for Optimism?: The Relationship Between Perceived Controllability and Optimistic Bias*, 15 J. SOC. & CLIN. PSYCHOL. 9, 11–12 (1996) (suggesting that perceived controllability and optimistic bias are associated); Cynthia T.F. Klein & Marie Helweg-Larsen, *Perceived Control and the Optimistic Bias: A Meta-Analytic Review*, 17 PSYCHOL. & HEALTH 437, 437–38 (2002) (investigating the linkage between perceived control association and optimistic bias by looking at twenty research studies).

39 Elizabeth M. Ozer & Albert Bandura, *Mechanisms Governing Empowerment Effects: A Self-Efficacy Analysis*, 58 J. PERSONALITY & SOC. PSYCHOL. 472, 472–73 (1990) (investigating the psychology of increased personal empowerment through a study of women enrolled in community self-defense programs).

access to their revealed information decrease, they demonstrate a greater extent of optimistic bias in privacy risk perceptions.

III. PRIVACY DECISION MAKING: RATIONAL CHOICE VS. BOUNDED RATIONALITY

A. Privacy Calculus

Within the robust body of research that attempts to understand individual privacy decision making, it has been found that the *calculus perspective* (i.e., economic cost-benefit analysis) of information exchange is "the most useful framework for analyzing contemporary consumer privacy concerns."[40] This perspective reflects an implicit understanding that privacy can be interpreted in "economic terms."[41] That is to say, "individuals should be willing to disclose personal information in exchange for some economic or social benefit subject to an assessment that their personal information will be subsequently used fairly and they will not suffer negative consequences in the future."[42] This calculus perspective of information exchange is especially apparent in recent research analyzing consumer privacy concerns.[43] That is to say, consumers often calculate the value of the benefit being offered in exchange for their personal information in the decision making process of an information disclosure.[44]

---

40 Mary J. Culnan & Robert J. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, 59 J. SOC. ISSUES 323, 326 (2003).

41 Peter H. Klopfer & Daniel I. Rubenstein, *The Concept* Privacy *and Its Biological Basis*, 33 J. SOC. ISSUES 52, 64 (1977) (discussing the degree to which privacy can be considered in terms of cost/benefit analysis).

42 Culnan & Bies, *supra* note 40, at 326–27.

43 *Id.* at 327; Mary J. Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10 ORG. SCI. 104, 104, 106 (1999) (hypothesizing that consumers will be more willing to disclose personal information to be used for marketing when their concerns about privacy are addressed by fair procedures); Han Li et al., *Understanding Situational Online Information Disclosure as a Privacy Calculus*, 51 J. COMPUTER INFO. SYS., Fall 2010, at 62 (testing how an individual's decision making on information disclosure is driven by competing situational benefits and risk factors).

44 Mary J. Culnan, *"How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use,* MIS Q., Sept. 1993, at 341, 344–45, 356 (measuring reactions towards use of personal information based on relative degrees of sensitivity to privacy); Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. PUB. POL'Y & MARKETING 149, 158, 161 (1991) (discussing willingness of consumers to disclose information for research purposes based on what they will receive in return); George R. Milne & Mary Ellen Gordon, *Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework*, 12 J. PUB. POL'Y & MARKETING 206, 206–07 (1993) (examining transactions in which consumers provide information about themselves in exchange for offers that may be of interest to them); Kim Bartel Sheehan & Mariea Grubbs Hoy, *Dimensions of*

Coherent with the essential ideas of the privacy calculus, the rational choice theory may further explain how individuals make decisions on information disclosure.[45] This theory suggests that individuals calculate the likely costs and benefits of any engagement before making a decision.[46] Individuals tend to pursue outcomes that maximize positive valences, which can be directly enhanced by benefits provided, and minimize negative valences.[47] Along the line of rational choice theory, a higher level of privacy concerns that are viewed as negative valences would be expected to negatively influence an individual's privacy decision making and subsequent information disclosure behavior.

B. Bounded Rationality

Although such a rational choice approach of analyzing privacy calculus has an intuitive appeal, recent studies have pointed out that users' actual privacy behaviors often fail to display the rational tradeoff that the privacy calculus model would suggest.[48] For example, through an experimental study, Berendt et al. demonstrated that users do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so.[49]

Acquisti and his colleagues have elaborated on this phenomenon of privacy paradox and argued that the dichotomy between privacy attitude and behavior is due to *bounded rationality*.[50] Because of the

---

Privacy Concern Among Online Consumers, 19 J. PUB. POL'Y & MARKETING 62, 63–64 (2000) (exploring influences on consumer privacy concerns).

45 JOHN VON NEUMANN & OSKAR MORGENSTERN, THEORY OF GAMES AND ECONOMIC BEHAVIOR ch. I (2d ed. 1947).

46 *Id.*

47 Culnan & Bies, *supra* note 40, at 327; Eugene Stone & Dianna L. Stone, *Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms*, 8 RES. PERSONNEL & HUM. RESOURCES MGMT. 349 (1990).

48 Carlos Jensen et al., *Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior*, 63 INT'L J.HUM.-COMPUTER STUDS. 203, 226 (2005) (discussing how frequently and significantly the rational-choice model fails in the privacy context); Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 101, 113, 116 (2007) (investigating the extent to which people intend to disclose and actually disclose personal details during marketing exchanges).

49 Bettina Berendt et al., *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, COMM. ACM, Apr. 2005, at 101, 102 ("Findings suggest that, given the right circumstances, online users easily forget about their privacy concerns and communicate even the most personal details without any compelling reason to do so.").

50 *See* Acquisti, *supra* note 2, at 3 ("[B]ounded rationality refers to the inability to calculate and compare the magnitudes of payoffs associated with various strategies the individual may choose in privacy-sensitive situations. It also refers to the inability to process all the

potential impacts of information processing capacity limitations and psychological distortions on individual decision making, human agents are unable to have absolute rationality.[51] As pointed out by Acquisti, the economic literature implies inconsistency of personal preference over time—future events may be discounted at different discount rates than near-term events.[52] Therefore, bounded rationality may affect privacy decisions: the benefits of disclosing personal information may be immediate (e.g., ease of contacting friends), but the risk of such information disclosure may be invisible or spread over future periods of time (e.g., identity theft).[53] Individuals may genuinely want to protect their information privacy, but because of bounded rationality, they may opt for immediate benefits of information disclosure, rather than carefully calculating long-term risks of information disclosure.[54]

Based on the above theoretical and empirical evidence, I argue that an individual's privacy decision making in the context of OSNs should encompass the notion of bounded rationality that captures the difference between *knowing* a privacy threat and *acting on* the privacy threat. Therefore, with the availability of immediate benefits in terms of self-presentation, relationship maintenance, extending social circles, and increasing popularity on OSNs, users are very likely to opt

---

stochastic information related to risks and probabilities of events leading to privacy costs and benefits."); Acquisti & Grossklags, *supra* note 5, at 26 ("The individual decision process with respect to privacy is affected and hampered by multiple factors. Among those, incomplete information, bounded rationality, and systemic psychological deviations from rationality suggest that the assumption of perfect rationality might not adequately capture the nuances of an individual's privacy-sensitive behavior.").

51 *See generally* HERBERT A. SIMON, 1 MODELS OF BOUNDED RATIONALITY, at xx (1984) (collecting the author's various essays on "economic subjects" which, he notes, are "sensitive to the limits of human rationality . . . [t]hat the concept of bounded rationality enters early in these essays should occasion no surprise").

52 *See* Acquisti, *supra* note 2, at 4 ("[I]ndividuals have a tendency to discount 'hyperbolically' future costs or benefits. In economics, hyperbolic discounting implies inconsistency of personal preferences over time—future events may be discounted at different discount rates than near-term events." (footnote omitted)).

53 *Id.* ("Hyperbolic discounting may affect privacy decisions, for instance when we heavily discount the (low) probability of (high) future risks such as identity theft."); Acquisti & Grossklags, *supra* note 5, at 31 ("Discounting might also affect privacy behavior . . . . If individuals have time inconsistencies . . . they might easily fall for marketing offers that offer low rewards now and a possibly permanent negative annuity in the future. Moreover, although they might suffer in every future time period from their earlier mistake, they might decide against incurring the immediate cost of adopting a privacy technology . . . even when they originally planned to.").

54 *See* Acquisti, *supra* note 2, at 4 ("[P]eople may genuinely want to protect themselves, but because of self-control bias, they will not actually take those steps, and opt for immediate gratification instead.").

for instant gratification by discounting the potential risks of information disclosure.

IV. PRIVACY MANAGEMENT STRATEGIES

In the privacy literature, privacy control mechanism has been mainly understood as the individual choice to opt-in or opt-out from firms' data collection activities,[55] or as the ability to decide how one's information is collected, used, and shared.[56] This body of literature's focus on *individual* privacy management, however, makes it too narrow, for it excludes those aspects of privacy management that are beyond individual choice. Schwartz questions whether individuals are able to employ meaningful information control in all circumstances, given discrepancies in knowledge and power in the process of data gathering and transfer.[57] The implication is that privacy management is not just a matter for the exercise of individual control but also an aspect of engineering innovation, group structure, organizational commitment, and social controls (e.g., legislation, regulation, and codes of conduct by professional associations).[58]

To provide a richer conceptual description, I apply the control agency theory in the psychology literature to the understanding of privacy management strategies. In particular, the control agency theory allows us to not only examine the effects of *personal control*, in which the self acts as the control agent to manage privacy, but also include *collective control* in which a social group acts as the control agent to manage privacy, as well as *proxy control* in which powerful

55 *See generally* Eve M. Caudill & Patrick E. Murphy, *Consumer Online Privacy: Legal and Ethical Issues*, 19 J. PUB. POL'Y & MARKETING 7, 7–19 (2000) (discussing privacy control on the Internet, especially regarding the choice to opt-in or out of control mechanisms).

56 *See* Naresh K. Malhotra et al., *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*, 15 INFO. SYS. RES. 336, 338 (2004) ("[A] firm's *collection* of personally identifiable information is perceived to be fair only when the consumer is granted *control* over the information and the consumer is *informed* about the firm's intended use of the information.").

57 *See generally* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1612 (1999) (arguing that "the lack of knowledge about personal data use allows the capture of information that might never be generated if individuals had a better sense of the Internet's data privacy zones").

58 *See* George Duncan, *Privacy by Design*, 317 SCI. 1178, 1178 (2007) ("To help balance privacy concerns and the need for personal data, a new paradigm is emerging, in which system designers conduct privacy risk assessments and incorporate privacy as a fundamental design parameter.").

others (such as government and industry regulators) act as the control agent to protect privacy.[59]

Three paths to protecting privacy can be identified from the control agency theory, which differentiates three types of privacy management strategies. First, perceived control can be raised by having personal control, where the agent of control is the individual.[60] Personal agency suggests that individuals are motivated to act upon opportunities that allow them to be the sole initiator of their behavior.[61] The second type of control is collective control, in which individual attempts to control the environment as a member of a group or collective.[62] In collective control, responsibility and agency will be diffused among all actors.[63]

Third, perceived control can be amplified by having *proxy control*, where the agent of control is powerful others.[64] In proxy agency, "people try by one means or another to get those who have access to resources or expertise or who wield influence and power to act at their behest to secure the outcomes they desire."[65]

The privacy literature describes three major approaches to help protect privacy: individual self-protection, collective privacy protection, and social controls through regulation and codes of conduct by

---

59 *See* Albert Bandura, *Social Cognitive Theory: An Agentic Perspective*, 52 ANN. REV. PSYCHOL. 1, 13 (2001) ("Social cognitive theory distinguishes among three different modes of human agency: personal, proxy, and collective."); *see also* Susumu Yamaguchi, *Culture and Control Orientations*, *in* THE HANDBOOK OF CULTURE AND PSYCHOLOGY 223 (David Matsumoto ed., 2001) (discussing the distinctions between "personal control," "proxy control," and "collective control").

60 *See* Bandura, *supra* note 59, at 10 ("Perceived self-efficacy occupies a pivotal role in the causal structure of social cognitive theory because efficacy beliefs affect adaptation and chance not only in their own right, but through their impact on other determinants." (citations omitted)); *see also* Ellen A. Skinner, *A Guide to Constructs of Control*, 71 J. PERSONALITY & SOC. PSYCHOL. 549, 558 (1996) (discussing the relationship between personal and perceived control).

61 *See* Bandura, *supra* note 59, at 6 ("[T]he power to originate actions for given purposes is the key feature of personal agency.").

62 *See* Yamaguchi, *supra* note 59, at 230 ("In *collective control*, one attempts to control the environment as a member of a group or collective, which serves as an agent of control.").

63 *See* Bibb Latané et. al., *Many Hands Make Light the Work: The Causes and Consequences of Social Loafing*, 37 J. PERSONALITY & SOC. PSYCHOL. 822, 823 (1979) ("Social impact theory holds that when a person stands as a target of social forces coming from . . . outside the group, the impact of these forces on any given member should diminish in inverse proportion to the strength, immediacy, and number of group members. Impact is divided up among the group members, in much the same way that responsibility for helping seems to be divided among witnesses to an emergency." (citations omitted)).

64 *See* Bandura, *supra* note 59, at 13 (discussing proxy control generally); Yamaguchi, *supra* note 59, at 228–30 ("*Proxy control* means control by someone else for the benefit of the person.").

65 Bandura, *supra* note 59, at 13.

professional associations.[66] Below I argue that these approaches fall into three generic categories based on the type of control agency they provide.

A. Individual Privacy Management

The first control-enhancing mechanism comprises tools and approaches that allow individuals to protect their information privacy by directly controlling the flow of their personal information to others. Individual privacy management is often viewed as a dynamic boundary regulation process, where individuals attempt to balance the privacy-publicity tradeoff among many different genres of information disclosure in order to assume the proper identity for a given audience.[67] The agent of control in individual privacy management is the self, and the effects of this mechanism arise due to the opportunity for personal control. When individuals exercise personal control through individual self-protection actions, they are striving for "primary control" over their environment.[68] Such a mechanism empowers individuals with primary control over how their personal information may be gathered by merchants and service providers.

In the context of OSNs, prior research describes two types of individual privacy management: behavioral self-protection and technological self-protection.[69] An array of behavioral self-protection approaches has been discussed in terms of choosing a private communication channel (e.g., private messages instead of wall posts on Facebook), using deliberate wordings and tones in (semi) public

66 H. Jeff Smith et al., *Information Privacy Research: An Interdisciplinary Review*, 35 MIS Q. 989, 1000–01, 1007 (2011) (discussing the relative merits of each approach to privacy protection).

67 *See* Mark S. Ackerman & Lorrie Cranor, *Privacy Critics: UI Components to Safeguard Users' Privacy*, *in* PROCEEDINGS OF THE 1999 ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI) 258, 258–59 (1999) (discussing privacy as "an information interface problem"); Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, *in* PROCEEDINGS OF THE 2003 ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI) 129, 131–32, 135 (2003) (discussing the "disclosure boundary" between "privacy and publicity" and the "identity boundary" between "self and other").

68 John R. Weisz et al., *Standing Out and Standing In: The Psychology of Control in America and Japan*, 39 AM. PSYCHOL. 955, 955–56 (1984) (discussing that the strategy of primary control is to "influence existing realities" and that the typical targets for causal influence include "environmental circumstances" (internal quotation marks omitted)).

69 *See* Hoadley et al., *supra* note 4, at 50–60 (2010) (exploring changes in Facebook users' attitudes towards privacy and behavior patterns in light of Facebook's News Feed and Mini Feed features); Anna C. Squicciarini et al., *CoPE: Enabling Collaborative Privacy Management in Online Social Networks*, 62 J. AM. SOC'Y INFO. SCI. & TECH. 521, 523–28 (2011) (proposing a technological mechanism to support joint management of shared shared content among users who post content in OSNs).

posts, avoiding publicizing content that could be problematic, deleting sensitive content (in one's profile and/or the comments one has posted elsewhere), untagging photos or place check-ins, and withholding sensitive information.[70]

Technological self-protection approaches comprise privacy-enhancing technologies ("PETs") that allow individuals to protect their privacy by directly controlling the flow of their personal information to others.[71] In the context of OSNs, to assuage user perceptions of privacy invasions, a number of social networking sites have been rolling out privacy control features that provide users with the means to control the disclosure, access, and use of their personal information.[72] Some social networking sites even embedded the privacy control features into the very use of various social networking functions and thus integrated privacy control as part of social networking functionality (e.g., creating social circles on Google+).[73] With various features that support the functions of specifying privacy preferences for using different applications on the OSNs, users are able to limit the amount of personal information disclosed on the OSNs. For example, Facebook users can specify their privacy preferences on who can see their profiles and personal information, who can search for them, how they can be contacted, what stories about them get published to their profiles, etc. In sum, these behavioral and technological privacy management strategies could provide users with the means and capabilities to control information release and limit information access by others and thus may reduce their perceptions of privacy risks.

B. Collective Privacy Management

The second control-enhancing mechanism is comprised of tools and approaches that allow individuals to protect privacy as a member of a group by harnessing group members' collective privacy know-

---

70 *See* Airi Lampinen et al., *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*, *in* PROCEEDINGS OF THE 2011 ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI) 3217, 3217–26 (2011) (identifying social networking site user concerns and exploring strategies available to users to allay and address these concerns).

71 Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY 125 (Philip E. Agre & Marc Rotenberg eds., 1997) ("PETs . . . seek to eliminate the use of personal data altogether or to give direct control over revelation of personal information to the person concerned.").

72 *See* Lampinen et al., *supra* note 70, at 3221–25 (2011) (discussing privacy control strategies on social networks generally).

73 *See A Quick Look at Google+*, GOOGLE, https://www.google.com/intl/en-US/+/learnmore/index.html#circles (last visited Feb. 14, 2012).

ledge and preferences to make informed privacy decisions together. When a user discloses her personal information in OSNs, the personal information moves to a collective domain where the user and her social ties become co-owners with joint responsibilities for keeping the information safe and private. Collective privacy management includes interpersonal actions and decisions associated with how information privacy is maintained by a group of individuals who co-manage that information. It differs from individual privacy management because of its change of agency (from the self to a group), its inclusion of interpersonal privacy decision making, and its co-management of shared information. Collective privacy management is seen as a process of maintaining social boundaries among many relationships that often overlap and becomes a group issue when the actions of one individual affect the privacy of another individual.

Prior literature on collective privacy management explores how different communication technologies—especially social networking websites—affect collective privacy boundary management among users who co-own and co-manage shared information. This stream of research often highlights the tension or conflict that an individual user faces when creating contents that may connect with others' identities (e.g., uploading an image about a friend, tagging a friend in an image, or linking to a friend's personal profile). Such collaborative activities raise a new set of privacy challenges because a person's private information can be easily revealed in content created by others. For example, a study of photo "tagging" and "untagging" on Facebook has exposed the complexities of collective privacy management, the tensions of content ownership, and the effects that one user uploading and tagging a picture of another can have on the latter's relationships with friends, family, employers, etc.[74]

Prior privacy research on OSNs describes behavioral and technological means for users to enact collective privacy practices for co-managing their shared information and content.[75] These collective privacy practices comprise strategies or tools that allow individuals and their social group members collectively acting as the control agents to exercise collective control over the flow of their shared in-

---

74 *See* Andrew Besmer & Heather Richter Lipford, *Moving Beyond Untagging: Photo Privacy in a Tagged World*, *in* PROCEEDINGS OF THE 28TH INTERNATIONAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI) 1563, 1568–71 (2010) (discussing the results of a study in which participants were asked to, among other things, "select a photo they did not want at least one other person to be able to see and untag or restrict that photograph on Facebook").

75 *Id.* at 1564; *see also* Lampinen et al., *supra* note 70, at 3217–19 (2011) (discussing various prior studies regarding social network privacy concerns and technology).

formation. Lampinen et al. identify behavioral strategies for users to collectively manage their shared information, e.g., negotiating and agreeing on "rules of thumb" concerning sharing with other users, asking for approval before disclosing content from those involved, and asking another person to delete content.[76]

In terms of technological strategies, researchers have begun proposing the PETs associated with collective privacy management. Technical solutions include addressing the conflicting privacy preferences among multiple content owners,[77] restricting shared content to a selected group of contacts,[78] proposing a user-centric privacy architecture to support collaborative privacy practices,[79] developing technical means to facilitate interactions among co-owners for co-managing shared content,[80] and promoting collaborative privacy awareness through facilitating a group's social collaborations in privacy decision making.[81] For instance, Besmer et al. proposed a friendship-based protection model which facilitates collective privacy management.[82] In their proposed solution, when a privacy-conscious user makes informed decisions for himself or herself, that privacy setting is in turn used to promote privacy awareness among his or her friends on the same network.[83] In sum, this stream of research ad-

---

76 Lampinen et al., *supra* note 70, at 3221–23.

77 *See* Anna C. Squicciarini et al., *Collective Privacy Management in Social Networks*, *in* PROCEEDINGS OF THE 18TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 521, 521–22 (2009) (discussing collaborative privacy management of shared content).

78 *See* Mohammad Mannan & Paul C. van Oorschot, *Privacy-Enhanced Sharing of Personal Content on the Web*, *in* PROCEEDINGS OF THE 17TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 487, 487–88 (2008) (discussing control mechanisms for partially restricting personal Web content).

79 *See* Jan Kolter et al., *Collaborative Privacy Management*, 29 COMPUTERS & SEC. 580, 581 (2010) (suggesting that a "collaborative privacy community facilitates Internet users to share privacy-related information about service providers").

80 *See* Squicciarini, *supra* note 69, at 523–28 (proposing a mechanism to support joint management of shared shared content among users who post content in OSNs).

81 *See* Andrew Besmer et al., *Social Applications: Exploring A More Secure Framework*, *in* PROCEEDINGS OF THE 5TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2009) (seeking to improve the current access control model used by application platforms so that protection is provided while still allowing desirable information access).

82 *Id.* at 3.

83 Taking the example from Besmer et al.'s work to illustrate their friendship-based solution: Bob (the target) is a careless user who does not pay close attention to protecting his profile privacy and leaves his default application policy to be very permissive. Alice (the viewer) is Bob's friend, and she installed a horoscope application which is not installed by Bob. Alice is security conscious and she set up her application policy to allow access to only the birth date attributes. The application will now only be able to access Bob's birth date when requested by Alice, and nothing more. Alice's awareness does not only protect her but it also protects Bob's profile due to the fact that Alice's policy is incorporated when the application attempts to access Bob's profile. *Id.*

dresses the interactional and collective aspects of privacy management, which could provide users with the means and capabilities to control information release and limit information access in a collective fashion, and thus may reduce their collective concerns for information privacy.

C. Proxy Privacy Management

When exercise of personal control is neither readily available nor encouraged, people might well relinquish their direct control preferences and seek "security in proxy control."[84] *Proxy control* is an attempt to align oneself with a powerful force in order to gain control through powerful others when people "do not have enough skills, knowledge, and power to bring about their desired outcome or avoid an undesired outcome in the environment . . . ."[85] In the privacy context, when users perceive that they lack the resources to directly control their personal information, they may reshape their decisions on information disclosure by considering the role of powerful others (e.g., legislators) who can act on their privacy benefits.[86] The third mechanism refers to proxy privacy management where powerful forces (i.e., legislators or industry self-regulators) act as the control agents for individuals to exercise proxy control over their personal information.

Prior privacy research describes two types of proxy privacy management: *industry self-regulation* and *government regulation*.[87] Industry self-regulation is a commonly used approach that consists of industry codes and self-policing trade groups and associations (e.g., Direct Marketing Association) as a means of regulating privacy practices. Seals of approval such as TRUSTe or certifications are other examples of mechanisms that are designed to confirm adequate privacy compliance.[88] Violation of the codes of conduct can mean revocation of the privacy seal, or referral to the law authority such as the appro-

---

84 Albert Bandura, *Self-Efficacy Mechanism in Human Agency*, 37 AM. PSYCHOL. 122, 142 (1982); Yamaguchi, *supra* note 59, at 228 (internal quotation marks omitted).

85 Yamaguchi, *supra* note 59, at 228–29.

86 *See* Heng Xu & Hock-Hai Teo, *Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective*, *in* PROCEEDINGS OF THE 25TH ANNUAL INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS 793, 797 (2004) (discussing the effects of proxy control in the context of location-based services ("LBS"): "when people perceive that they lack the requisite resources to directly control their personal information disclosed for LBS transactions, they may reshape their decision on using LBS by considering the availability of powerful others who can be induced to act for their benefit").

87 *Id.*

88 *Id.*

priate attorney general's office or the Federal Trade Commission ("FTC").[89]

In the privacy literature, the presence of privacy seals have been found to have a positive effect on the perception of trust in a company,[90] resulting in more favorable perceptions toward the privacy statement.[91] However, a number of recent studies uncovered insufficient enforcement power by third-party certification agencies to ensure firms act according to their privacy policies. Miyazaki and Krishnamurthy reviewed sixty high-traffic websites and found no support for the hypothesis that participation in a seal program is an indicator of better privacy practices.[92]

Government regulation is another mechanism that relies on the judicial and legislative branches of a government to set and enact laws for privacy protection.[93] The privacy protection standards set by the government enable individuals to believe that firms will protect privacy post-contractually, thereby providing individuals with a sense of control over their personal information.[94] Milberg, Smith, and Burke conducted a survey of 595 internal auditors of the Information Systems Audit and Control Association ("ISACA") from nineteen different countries and suggested that, when corporations exhibit loose management of information privacy, and/or when individual privacy concerns rise, individuals are more inclined to prefer government in-

89 Paola Benassi, *TRUSTe: An Online Privacy Seal Program*, COMM. ACM, Feb. 1999, at 56, 58–59.

90 Nora J. Rifon et al., *Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures*, 39 J. CONSUMER AFF. 339, 340 (2005) ("Partipants had more favorable perceptions of privacy policies at Web sites that displayed seals . . . .").

91 Anthony D. Miyazaki & Sandeep Krishnamurthy, *Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions*, 36 J. CONSUMER AFF. 28, 42 (2002) (suggesting the "presence of the Internet seal of approval logo was shown to raise consumer perceptions of the favorableness of a firm's privacy-related practices").

92 *Id.* at 36–37; *see also* Robert LaRose & Nora Rifon, *Your Privacy is Assured—of Being Disturbed: Websites With and Without Privacy Seals*, 8 NEW MEDIA & SOC'Y 1009, 1023 (2006) (noting the irony that some studied websites which "publicize[d] their concern for consumer privacy by displaying privacy seals were actually more likely to infringe upon their visitors' privacy").

93 Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3–19 (William Daley & Larry Irving eds., 1997) (outlining possible alternatives for protection of personal information).

94 Zhulei Tang et al., *Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or* Caveat Emptor, 24 J. MGMT. INFO. SYS. 153, 159 (2008) (arguing caveat emptor, combined with government regulation of deceitful claims, will succeed in increasing privacy protection).

tervention and be distrustful of firm self-regulation.[95] At the society level, Tang et al. indicate that, although legislations can generally enhance consumer trust, government interventions may not be socially optimal in all situations because of lower revenue margins for companies and higher costs for consumers.[96] Thus, promoting individual and collective privacy management strategies in the context of OSNs might be increasingly perceived as a viable substitute for proxy privacy management approach because of the flexibility to cross international and regulatory boundaries.

V. IMPACTS OF TRUST

A. Trust in Providers of OSNs

The conceptual academic literature in consumer privacy indicates that the Integrative Social Contract Theory ("ISCT")[97] is particularly appropriate for understanding the tensions between firms and consumers over information privacy.[98] According to this ISCT perspective, "[a] social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behavior of those involved."[99] When consumers provide personal information to a company and the company in turn offers some benefits to the consumer, one generally understood obligation accruing from entering into this social contract is that the firm will

95 Sandra J. Milberg et al., *Information Privacy: Corporate Management and National Regulation*, 11 ORG. SCI. 35, 42–47 (2000) ("[I]f corporations exhibit loose management of information privacy, then individuals are more likely to call for strong privacy laws rather than allowing corporations to self-regulate . . . .").

96 Tang et al., *supra* note 94, 154–68 (suggesting government regulation is more effective but less efficient and not optimal for society).

97 THOMAS DONALDSON & THOMAS W. DUNFEE, TIES THAT BIND: A SOCIAL CONTRACTS APPROACH TO BUSINESS ETHICS (1999) (explaining the Integrative Social Contract Theory).

98 Eve M. Caudill & Patrick E. Murphy, *Consumer Online Privacy: Legal and Ethical Issues*, 19 J. PUB. POL'Y & MARKETING 7, 8, 12 (2000) ("[C]onsumers have varying degrees of concern with privacy and place different values on their personal information" and "businesses do not always compete with consumers' best interests in mind."); Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing*, J. DIRECT MARKETING, Spring 1995, at 10, 11 ("Integrative social contact theory (ICST) provides a means for understanding the current tensions between marketers and consumers over privacy."); Milne & Gordon, *supra* note 44, at 212–14 (evaluating proposals to protect personal information of customers in direct mailing).

99 Caudill & Murphy, *supra* note 98, at 14.

undertake the responsibility to manage consumers' personal information properly.[100]

> This [implied social] contract is considered breached if consumers are unaware information is being collected, if the marketer rents the consumer's personal information to a third party without permission, or if consumers are not given an opportunity to remove their names from lists or otherwise restrict the dissemination of personal data about them,[101]

or their information is being shared, or their information is being used for other purposes.[102]

Thus, the social contract on information collection and use requires consumers' trust on the company's compliance with this social contract.[103] In the context of OSNs, because of the absence of assurances that the OSN providers will not engage in opportunistic behaviors in terms of information misuse, trust in an OSN provider is crucial in helping users overcome their perceptions of uncertainty. If the OSN provider is perceived to be caring about users' information privacy needs (perceptions of the "benevolence" of the provider), honest and consistent in its dealing with users' personal information (perceptions of the "integrity" of the provider), and capable of pro-

---

100 *Id.; see also* Culnan, *supra* note 98, at 11 ("When direct marketing is viewed as an implied social contract, consumers provide personal information in exchange for receiving solicitations and other information, based on an expectation that their personal information will be managed responsibly."); George R. Milne, *Consumer Participation in Mailing Lists: A Field Experiment*, 16 J. PUB. POL'Y & MARKETING 298, 298, 301 (1997) ("[A] social contract occurs when a customer provides a marketer with personal information at the point of purchase with the intention that the marketer will use this information to serve the customer better" and "a consumer's control over his or her personal information is a fundamental component of a fair implied social contract."); Milne & Gordon, *supra* note 44, at 207 ("To enter a social contractual relationship with an organization . . . consumers must perceive that the benefits of doing so outweigh the costs."); Phelps et al., *supra* note 15, at 29 ("[M]arketers should view consumers' exchange of information as an implied social contract." (citations omitted)).

101 Phelps et al., *supra* note 15, at 29.

102 Culnan, *supra* note 98, at 11–12 ("[I]f a marketer's practices do not reflect 'knowledge, notice, and no,' the result may be viewed as a consumer information problem."); Milne, *supra* note 100, at 298 ("If the marketer, however, rents the customer's personal information to a third party without permission, and the third party sends the customer unwanted solicitations, this could be a breach of the implied social contract.").

103 Caudill & Murphy, *supra* note 98, at 14–15 (discussing social contract theory in the context of direct marketing on the Internet); Culnan & Bies, *supra* note 40, at 327 ("[C]reating willingness in consumers to disclose personal information requires that the second exchange be based on a fair social contract. Developing information practices that address the perceived risk of disclosure should result in positive experiences with the organization over time, increasing the consumer's perceptions that the organization can be trusted." (citations omitted)); Donna L. Hoffman et al., *Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web*, 15 INFO. SOC'Y 129, 133 (1999) (comparing social exchange to economic exchange and asserting that social exchange tends to invoke feelings of trust).

tecting their personal information (perceptions of the "competence" of the provider), the level of concern over information privacy may be reduced.[104]

An OSN provider's interventions with regard to joining privacy seal programs and introducing privacy-enhancing features, therefore, should directly build users' trusting beliefs toward the OSN provider because of the nontrivial investment of time and resources made by the OSN provider to design, develop, and implement these privacy-enhancing initiatives. These actions should be interpreted as a signal that the OSN provider is actively addressing users' privacy concerns and will comply with the social contract by undertaking the responsibility to manage users' personal information properly. In other words, a particular OSN provider's privacy interventions (e.g., introduction of the privacy enhancing features and joining privacy seal programs) may increase users' trusting beliefs in an OSN provider.

B. Trust in Social Ties

Besides trust in the OSN provider (e.g., Facebook), Hoadley et. al also highlight the importance of trust in social ties (e.g., "friends," "friends of friends" on Facebook, and the university's Facebook users) in their case analysis of the Facebook News Feed privacy outcry.[105] When a user discloses her personal information in OSNs, the personal information moves to a collective domain where the user and her friends in OSNs become co-owners with joint responsibilities for keeping the information safe and private.[106] Individuals/friends on the user's contact list usually have a certain amount of information access to the user's profile and personal information may be misused if the relationship changes. In addition, it has been recently reported that personal details of Facebook users could potentially be breached due to their friends adding applications.[107] That is to say, even if

---

104 D. Harrison McKnight et al., *The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model*, 11 J. STRATEGIC INFO. SYS. 297, 303 (2002) (footnote omitted) (defining "trusting beliefs" as "integrity (trustee honesty and promise keeping), benevolence (trustee caring and motivation to act in the trustor's interests), competence (ability of the trustee to do what the trustor needs), and predictability (consistency of trustee behavior)").

105 *See generally* Hoadley et al., *supra* note 4, at 58 (noting the "importance of *perceived control* and *ease of information access* in alleviating users' privacy concerns . . .").

106 SANDRA PETRONIO, BOUNDARIES OF PRIVACY 10 (2002) ("When we are told private information by others, we enter into a contract of responsibility to be co-owners of the information.").

107 Wang et al., *supra* note 3, at 8 (suggesting "the ability for an application to gather information about one's friends should be another issue to be addressed. . . . If the user is not

some users think they have tight privacy and security settings, their personal information could be accessed and used by third-party applications due to their friends' ignorance of privacy and security.[108] The need for trust in social ties arises due to the inability to monitor other members on the network and uncertainty about their behaviors. Trust in social ties, therefore, could be an effective mechanism to reduce the complexity of human conduct in situations where people have to cope with uncertainty.[109] Such trusting belief in social ties may enable users to perceive that their personal information will be co-managed appropriately by their "friends."

VI. DISCUSSION AND CONCLUDING COMMENTS

Although terms such as "invasion of privacy" and/or "privacy breach" have been considerably hyped in the media, conceptualizations of information privacy in the context of OSNs have been somewhat patchy. In the privacy literature, there are some difficulties in identifying common ground of information privacy, and this challenge will likely become more pronounced in the next few years. According to a 2007 study sponsored by the National Research Council, the relationship between information privacy and society is now under pressure due to several factors that are "changing and expanding in scale with unprecedented speed in terms of our ability to understand and contend with their implications to our world, in general, and our privacy, in particular."[110] Factors related to technological change (e.g., cloud computing) and to societal trends (e.g., globalization and cross-border data flow) are combining to force a reconsideration of basic privacy concepts and their implications.[111] Therefore, rather than drawing on a single theoretical lens, this Article builds upon previous literature from multiple theoretical lenses to create a common understanding of Privacy 2.0 in the context of OSNs. A theoretical framework was proposed to synthesize results of prior privacy studies, and to outline major research issues (see *infra* Figure 1).

---

diligent about setting secure privacy settings, the apps may be able to access his/her friends' information.").

108 *Id.*

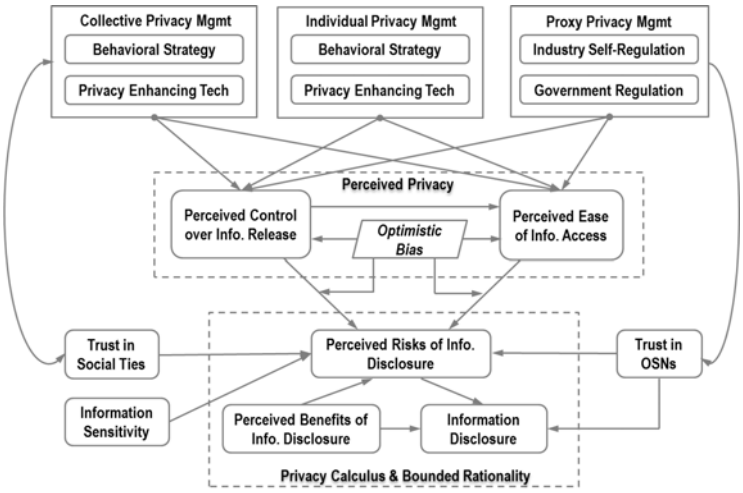
109 Niklas Luhmann, *Familiarity, Confidence, Trust: Problems and Alternatives*, *in* TRUST 94, 97 (Diego Gambetta ed., 1988) ("Trust . . . presupposes a situation of risk. . . . You can avoid taking the risk, but only if you are willing to waive the associated advantages. You do not depend on trusting relations in the same way you depend on confidence, but trust too can be a matter of routine and normal behaviour.").

110 COMM. ON PRIVACY IN THE INFO. AGE, *supra* note 20, at 27.

111 *Id.* at 28 (presenting a chart summarizing large-scale factors affecting privacy).

FIGURE 1

PROPOSED THEORETICAL FRAMEWORK



The proposed framework integrates the control agency theory and identifies three privacy management strategies by linking them with different types of control agencies: individual, proxy, and collective privacy management in the context of OSNs. Exploration of the influences and outcomes of users' perceived privacy is particularly important in discussing the effectiveness of privacy management strategies, as these are often confused in technical design, OSN providers' data collection practices, and users' privacy expectations. This Article argues that an individual's perceived privacy is better viewed as perceived control over information release and perceived ease of information access, with the considerations of optimistic bias. Due to the effect of optimistic bias, users would tend to magnify the degree of control involved in the release of their personal information, while they often underestimate the degree of information access by others. The impact of optimistic bias on risk perceptions of information disclosure should also not be discounted. Users on OSNs tend to demonstrate a tendency to believe that their risk levels are lower than that of their peers.

According to the calculus lens of privacy, individuals can be expected to be rational in dealing with information sharing. Rationality dictates that users will reveal their personal information as long as they perceive benefits will exceed the risks of information disclosure. The theoretical lens of privacy calculus highlights the importance of risk appraisal and benefit calculation in an individual's information

disclosure behavior. However, according to the economics literature, human agents are unable to have absolute rationality because of the potential impacts of information processing capacity limitations and psychological distortions on individual decision making. Users may genuinely want to protect their personal data, but because of bounded rationality, rather than carefully calculating long-term risks of information disclosure, they may opt for immediate gratification instead.

Other rational factors such as trust and information sensitivity should also be considered as important determinants of information withholding and information disclosure. Complete information disclosure can be expected when users trust the organization's benevolence, integrity, and competence to protect their information. It has been suggested in the privacy literature that information sensitivity (i.e., the type of personal information requested by an organization) could also influence users' decisions to withhold or disclose their personal information.[112] Information such as financial data, medical records, and personal identifiers (e.g., social security numbers) was found to be much more sensitive than demographic characteristics, purchase behavior, and lifestyle habits.[113]

In conclusion, the main contribution of this Article is the generation of a privacy conceptual framework in the domain of OSNs, with rich grounding in a range of multidisciplinary privacy literatures in behavioral sciences, information systems, public policy, and social psychology. Privacy researchers who are interested in the domain of OSNs are likely to benefit from the theoretical framework proposed in this Article. It identifies the factors affecting users' decisions to withhold and disclose information and how their privacy decision making is influenced by these factors. Presenting a multidisciplinary synthesis, the framework developed in this Article should be of interest to academic researchers, providers of OSNs, legislators, industry self-regulators, and designers of privacy-enhancing technologies.

---

112 Malhotra et al., *supra* note 56, at 342 ("It is known that consumers' reactions to privacy threats depend on the type of information requested by marketers. All things being equal, releasing more sensitive information is perceived as more risky than releasing less sensitive information." (citations omitted)); Phelps et al., *supra* note 15, at 27 (considering the "types of personal information consumers are most and least willing to provide to direct marketers and other retailers").

113 *Id.* at 38 ("Consumers are least willing to provide financial and personal identifier information . . . . [M]ost respondents were willing to provide demographic, media, and lifestyle information . . . .").